UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/058,213	01/29/2002	Robert Lambert	00001-0425	2202

27871 7590 12/12/2005

BLAKE, CASSELS & GRAYDON LLP
BOX 25, COMMERCE COURT WEST
199 BAY STREET, SUITE 2800
TORONTO, ON M5L 1A9
CANADA

EXAMINER	
ABRISHAMKAR, KAVEH	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 12/12/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/058,213	LAMBERT ET AL.	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 September 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed on September 19, 2005. Claim 1 was originally received for consideration. Per the received amendment, claims 2-8 were added and claim 1 was amended. Claims 1-8 are currently being considered.

Response to Arguments

2. Applicant's arguments with respect to claim 1 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claims 2-3 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. The specification does not mention the steps i-l, which comprise a "third exponent", a

"fourth exponent" or a "second simultaneous exponentiation." For the purposes of examination, the claim is being treated as analogous to claim 1.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vanstone et al. (U.S. Patent 5,889,865) in view of Clapp (U.S. Patent 5,987,131).

Regarding claim 1, Vanstone discloses:

A method of generating a shared key by a first correspondent, wherein said key is computable by a second correspondent, said method comprising the steps of:

(a) "***said first correspondent making a first short term public key available to said second corespondent over a communication channel***" (column 7 lines 39-42);

(b) "***said first correspondent obtaining a second short term public key from said second correspondent***" (column 7 lines 39-42);

(c) "***said first correspondent computing a first exponent derived from a first short term private key, said first short term public key, and a first long term private key***" (column 7 lines 40-47);

(d) "***said first correspondent computing a second exponent derived from said first short term private key, said first short term public key, a second short term public key and said first long term private key***" (column 7 lines 40 – 47).

Vanstone does not explicitly mention the use of simultaneous exponentiation to generate a shared key. Clapp uses as table of different widths to establish a key (column 3 lines 55-67), which is established in dependent claims 4-5 as being the simultaneous exponentiation. Clapp and Vanstone are analogous arts as both pertain to key agreement protocols. It would have been obvious to use the a table generated from the public keys as disclosed by Clapp (see Abstract and column 3 lines 55-67), because it provides for "efficient and secure key exchange between two parties, both of whom have limited memory and computational resources" (column 3 lines 5-10), and further, "to reduce susceptibility to timing attacks while maintaining computational efficiency" (column 3 lines 22-27). Therefore, it would have been obvious to one of ordinary skill in the art to use the tables of exponents of Clapp with the key agreement protocol of Vanstone to increase the computational efficiency while reducing the susceptibility to timing attacks.

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Vanstone discloses:

The method of claim 1 further comprising the steps of:

g) said second correspondent making said second short term public key available to said first correspondent over said communication channel (column 7 lines 39-42);

h) said second correspondent obtaining said first short term public key from said first correspondent (column 7 lines 39-42);

i) said second correspondent computing a third exponent derived from a second short term private key, said second short term public key, and a second long term private key (column 7 lines 40-47);

j) said second correspondent computing a fourth exponent derived from said second short term private key, said second short term public key, said second long term private key, and said first short term public key (column 7 lines 40 – 47).

Vanstone does not explicitly mention the use of simultaneous exponentiation to generate a shared key. Clapp uses as table of different widths to establish a key (column 3 lines 55-67), which is established in dependent claims 4-5 as being the simultaneous exponentiation. Clapp and Vanstone are analogous arts as both pertain to key agreement protocols. It would have been obvious to use the a table generated from the public keys as disclosed by Clapp (see Abstract and column 3 lines 55-67),

because it provides for "efficient and secure key exchange between two parties, both of whom have limited memory and computational resources" (column 3 lines 5-10), and further, "to reduce susceptibility to timing attacks while maintaining computational efficiency" (column 3 lines 22-27). Therefore, it would have been obvious to one of ordinary skill in the art to use the tables of exponents of Clapp with the key agreement protocol of Vanstone to increase the computational efficiency while reducing the susceptibility to timing attacks.

Claim 3 is rejected as applied above in rejecting claim 2. Furthermore, Vanstone discloses:

The method of claim 2 wherein steps a) and g) are performed in parallel, steps b) and h) are performed in parallel, steps c) and d) are performed in parallel with steps i) and j), and steps k) and l) are performed in parallel with steps e) and f) (column 7 lines 39-47).

Claim 4 is rejected as applied above in rejecting claim 1. Vanstone does not explicitly disclose a simultaneous exponentiation wherein the simultaneous exponentiation comprises establishing a window of width w, and establishing a table of exponentiations using the short term and long term public key, and calculating a shared key. Clapp uses as table of different widths to establish a key (column 3 lines 55-67). Clapp and Vanstone are analogous arts as both pertain to key agreement protocols. It would have been obvious to use the a table generated from the public keys as disclosed by Clapp

(see Abstract and column 3 lines 55-67), because it provides for "efficient and secure key exchange between two parties, both of whom have limited memory and computational resources" (column 3 lines 5-10), and further, "to reduce susceptibility to timing attacks while maintaining computational efficiency" (column 3 lines 22-27). Therefore, it would have been obvious to one of ordinary skill in the art to use the tables of exponents of Clapp with the key agreement protocol of Vanstone to increase the computational efficiency while reducing the susceptibility to timing attacks.

Claim 5 is rejected as applied above in rejecting claim 4. Vanstone does not explicitly disclose that the examining of the tables includes retrieving the corresponding powers of values of said second short term public key and said second long term public key, accumulating the product of the entries, and squaring the product w times, and further examining the windows until a shared key is calculated. Clapp uses as table of different widths to establish a key (column 3 lines 55-67). Furthermore, Clapp squares and multiplies the entries (public keys) until the entries picked from the table equal the computation budget (width) to generate a secret key (column 3 lines 43-67). Also, Clapp discloses that uniformly distributed random keys can be generated by using the calculation sequences that include squaring the entries and placing them in an accumulator (column 4 lines 23-43). Clapp and Vanstone are analogous arts as both pertain to key agreement protocols. It would have been obvious to use the a table generated from the public keys as disclosed by Clapp (see Abstract and column 3 lines 55-67), because it provides for "efficient and secure key exchange between two parties,

both of whom have limited memory and computational resources" (column 3 lines 5-10), and further, "to reduce susceptibility to timing attacks while maintaining computational efficiency" (column 3 lines 22-27). Therefore, it would have been obvious to one of ordinary skill in the art to use the tables of exponents with squaring and accumulating of the entries, of Clapp with the key agreement protocol of Vanstone to increase the computational efficiency while reducing the susceptibility to timing attacks and generating uniformly generated random keys (column 4 lines 13-15).

Claim 6 is rejected as applied above in rejecting claim 1. Vanstone does not explicitly disclose that simultaneous exponentiation is performed by storing values of first and second exponents in registers, using pointers to accumulate and multiply corresponding values, and repeating the process until a shared key is computed. Clapp discloses multiplying previous value of the accumulator and placing this result in an accumulator, and after each calculation storing the output value in a register, where the value will be loaded for more calculation sequences until the computational budget is met and a shared key is computed (column 4 liens 31-53). Clapp and Vanstone are analogous arts as both pertain to key agreement protocols. It would have been obvious to use the a table generated from the public keys as disclosed by Clapp (see Abstract and column 3 lines 55-67), because it provides for "efficient and secure key exchange between two parties, both of whom have limited memory and computational resources" (column 3 lines 5-10), and further, "to reduce susceptibility to timing attacks while maintaining computational efficiency" (column 3 lines 22-27). Therefore, it would have been obvious

to one of ordinary skill in the art to use the tables of exponents with squaring and accumulating of the entries, of Clapp with the key agreement protocol of Vanstone to increase the computational efficiency while reducing the susceptibility to timing attacks and generating uniformly generated random keys (column 4 lines 13-15).

Claim 7 is rejected as applied above in rejecting claim 1. Furthermore, Vanstone discloses:

The method of claim 1 implemented in an elliptic curve cryptosystem (column 7 lines 62-67).

Claim 8 is rejected as applied above in rejecting claim 7. Vanstone does not explicitly disclose a simultaneous exponentiation wherein the simultaneous exponentiation comprises establishing a window of width w, and establishing a table of exponentiations using the short term and long term public key, and calculating a shared key. Clapp uses as table of different widths to establish a key (column 3 lines 55-67). Clapp and Vanstone are analogous arts as both pertain to key agreement protocols. It would have been obvious to use the a table generated from the public keys as disclosed by Clapp (see Abstract and column 3 lines 55-67), because it provides for "efficient and secure key exchange between two parties, both of whom have limited memory and computational resources" (column 3 lines 5-10), and further, "to reduce susceptibility to timing attacks while maintaining computational efficiency" (column 3 lines 22-27). Therefore, it would have been obvious to one of ordinary skill in the art to use the tables

of exponents of Clapp with the key agreement protocol of Vanstone to increase the computational efficiency while reducing the susceptibility to timing attacks.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Primary Examiner
AU 2131
12/7/05

KA
12/06/2005